U.S. Intellectual Property Protection in the Blockchain Industry: Trends and Solutions

By Matthew R. Schantz and Jeffery T. Gorham

Blockchains and cryptocurrencies have been experiencing booming growth. In the nine short years since the Bitcoin Whitepaper and open-source software implementation were released in 2008 and 2009, respectively, approximately 1,600 new cryptocurrencies have been created, representing approximately $300 billion (USD) in market capitalization.[1] The collective innovations therein show great promise to enhance many other industries. If organizations are not careful, though, myths, misconceptions, and blockchain-industry-specific pitfalls will undercut the opportunities they have to develop and commercialize intellectual property (IP) in this market.

Organizations in the blockchain industry, with their brilliant software developers often operating on bootstrapped budgets, frequently seek to minimize costs in several areas, especially legal costs. In this environment, IP practitioners will not be surprised to hear that blockchain organizations are employing questionable practices based on some old but lingering fallacies about IP law. Although catastrophic results might be avoided early on, damage from these penny-pinching practices can turn disastrous if left unchecked. On the other hand, zealously seeking IP protection may seem natural from an IP practitioner's perspective, but such a strategy can have unintended consequences that clash with client objectives, even attracting unwanted regulatory enforcement.

This article explores some nuances for intellectual property practitioners to consider and common misunderstandings practitioners may have to overcome when advising blockchain-based organizations concerning IP protection and risks.

Patents and Blockchain Technology

The original bitcoin technology was described in a 2008 publication and implemented in code released publicly in 2009. The code is available under the permissive "MIT" open-source license, and no patent owner has made claim to that technology. It therefore appears that this basic system is available on favorable terms for implementation in other systems. That being said, there have been huge opportunities for developers to build on this technology to solve many business and technical issues and apply to patent any improvements made. Of course, the Patent Office does not just issue a patent on every application, so the intersection of blockchain-based organizations and the patent world is worthy of some discussion.

Patent-Related Challenges

One patent-related challenge that blockchain-based organizations face is the combined newness and extreme popularity of the technology. Significant obstacles make it difficult—if not impossible—to determine with a reasonable amount of searching what technology is publicly known or already the subject of a patent application. The most notable of these confounding factors are that there are so many organizations in early stages of development, many with but a trivial public presence, while vocabulary around blockchain-related concepts is just being defined, and most patent applications are only made public 18 months after filing. Without a reliable way to determine what is publicly known, it is impossible to evaluate with certainty whether any given technology is novel or nonobvious over the prior art. Thus, the potential value of the patent on new blockchain technology must be discounted by the possibility that some unknown source has already made that technology public.

Matthew R. Schantz

Jeffery T. Gorham

Another challenge relates to the uncertain contours of patentable subject matter as applied to inventions implemented in software. Patent applications claiming such inventions face a high level of scrutiny after the U.S. Supreme Court's decision in *Alice Corp. v. CLS Bank International*.[2] In *Alice*, the Court held that claims to a computer-implemented algorithm used to facilitate financial escrow transactions were not directed to patentable subject matter because they attempted to cover a mere implementation of an abstract idea and failed to transform that abstract idea into a patent-eligible invention with "something more."[3] Although the *Alice* opinion did not *explicitly* rule that software patents are not patentable, the Court cited its opinions in previous case law[4] for the position that "a fundamental economic practice long prevalent" in an industry is not patentable subject matter, even if it is implemented via a computer, unless there is a "new and useful" application of, or improvement on the idea. Therefore, an invention that merely uses software to implement an abstract idea, or to implement a practice that is already used in a particular industry, is not patentable; only claims to recite "new and useful" implementa-

tions or improvements of those ideas can achieve patent protection.[5]

Subsequent cases that have applied and interpreted *Alice* have come to a variety of conclusions.[6] Recently, the inventions claimed in successfully defended patents improve how computers work at the technical level[7] or use technical means to solve technical problems.[8] Simply applying well understood computing technology to implement concepts that are well understood in the off-line world has been rejected as unpatentable subject matter. In the context of blockchain technology, this means that innovations to blockchain technology itself, applications of blockchain technology that quantifiably improve how computers work or work together, and applications of blockchain technology to existing systems that do more than simply implement database functions in a blockchain context might have a shot at success. In contrast, it would be hard to imagine an examiner or other fact-finder finding patentable subject matter in novel economic systems for exchanging rights through a cryptocurrency, or in mediating traditional economic arrangements with a blockchain-based token. Between those two extremes, the terrain is still uncertain.

Patent Applications

So, what is a blockchain-based organization to do? Under our current first-inventor-to-file regime,[9] any organization hoping to obtain patent protection should connect early with a patent attorney who understands the space. A provisional patent application can save the inventor's place in line at the Patent Office, protecting an applicant from later filers without the need for all of the formalities of a nonprovisional application or even the scope-defining "claims." Then, up to a year later, the applicant can file the nonprovisional application, getting the benefit of the provisional application's filing date as to everything disclosed therein, but hopefully with more complete development, a better view of what aspects of the invention are worth trying to protect, and even better funding. The claims and even the description should be carefully crafted to maximize the likelihood of success given the amorphous state of the law of patentable subject matter discussed above.

Defensive Publication

Even if the organization decides not to try to patent its innovations, it could still face patent infringement risk. Publishing a technical white paper might mitigate that risk, at least as to patent applications filed after that publication. To ensure that any patent application filed *after* the publication would not be able to cover anything that was sufficiently disclosed *in* the publication, such a paper should describe the organization's system in enough detail that one could read the paper and build a system. The organization would also need to make the publication well documented and public enough to be indexed and findable. Note, however, that defensive publication of a white paper could not remove the risk of infringing patents on earlier filed applications or protect aspects of the implementation that are not disclosed in the white paper.

Copyright Protection on Blockchain Applications and White Papers

A developer's white paper and computer code are typically protected by copyright as soon as they are written, as copyright in a creative work of authorship automatically springs into existence (with a very low threshold for creativity), and there is no registration requirement for copyright protection in the U.S. Any original work of authorship, such as a white paper or computer code, is covered by copyright at the moment it is "fixed in any tangible medium of expression."[10] One of several caveats for the "originality" requirement, however, is that a derivative work, or a work that is based upon one or more preexisting works,[11] only enjoys protection of the contributions from the new author, i.e., the derivative author's own original expression.[12]

"Given the much greater cost to file patent applications, this practice subsequently spread to the patent industry."

Of course, then, any white paper or blockchain code that the organization uses as a resource for its own development may be covered by copyright owned by many different authors, each of whom contributed part of the source work. Fortunately, a great deal of blockchain source code has been released under generous open-source licenses, reducing the risk of copyright infringement liability for the organization. The same is not true of white papers, so to minimize infringement risk, organizations should write their whitepapers from scratch.

Industry Trend: Using Outside Developers to Develop Technology

New organizations and their leadership often do not possess the deep understanding of blockchain coding needed to implement their ideas. As a solution, many organizations rely on outside developers who *do* understand the technology, bringing on these outside developers as independent contractors. As part of this process, many organizations ask that the developer sign a nondisclosure agreement and/or an independent contractor agreement that members of the organization drafted in-house, often from one or more templates which the organization found online after a cursory Google search. This is troublesome for many reasons.

Non-Disclosure Agreements are used predominantly to protect trade secrets and potential patent rights and to prevent a receiving party from sharing a disclosing party's trade secrets to other parties. Although this sounds like a good way to protect the organization in its interactions with outside developers, a traditional NDA does nothing to effectuate an assignment or transfer of IP rights from a developer to the organization, or to set-forth that such developed IP will be considered a "work made for hire," and therefore the exclusive property of the organization. Simply put, this industry practice is insufficient to fully protect an organization's IP interests.

Independent Contractor Agreements come closer to protecting an organization's IP interests. Independent Contractor Agreements should set forth the clear understanding that the developer is an independent contractor, that the developed work will be considered a "work made for hire" and therefore the sole and exclusive property of the organization, and, in the event that the IP is not considered a work made for hire, that the developer agrees to *and presently assigns*[13] any rights he or she may have in the developed work to the organization. Rights in inventions that the developer invents during the engagement should also be assigned to the organization in the Independent Contractor Agreement. Like the non-disclosure agreements discussed above, when organizations attempt to draft these agreements in-house they generally fail to draft the IP assignment or work-made-for-hire provisions to fully protect the organization.

Industry Trend: Posting a White Paper or Code to Seek "Poor-Man's" (Copyright/Patent) Protection

Many practitioners will be familiar with the various forms of "poor-man's copyright." This mythical creature usually constitutes a developer sending a copy of their work in a sealed, self-addressed, stamped envelope back to themselves via certified mail or other means, in order to have some evidence of authorship and defend oneself from future infringement claims. This is often attempted in order to avoid the trouble of registering the work with the U.S. Copyright Office.[14] However, no provision in the U.S. Copyright code allows a poor-man's copyright to substitute for registration,[15] and although courts have discussed matters related to a poor-man's copyright, no court has yet endorsed the practice as substitute for formal registration of a copyrighted work.[16]

Given the much greater cost to file patent applications, this practice subsequently spread to the patent industry.[17] Not surprisingly, mailing a disclosure to oneself does not secure for the inventor the exclusive rights that come with a patent granted by the U.S. Patent and Trademark Office (USPTO). Further, reliance on a poor-man's patent can be disastrous for developers, as it yields neither the benefit of an actual patent application (the possibility that the USPTO will grant a patent on the invention) nor protection against subsequent filings on the invention by others, as the first inventor to file an application wins over subsequent filers under the America Invents Act ("AIA") since the U.S. became a first-inventor-to-file country on March 16, 2013.[18]

The blockchain industry has seen its own iteration of the poor man's patent/copyright, where a developer will post the organization's white paper on a publicly visible website, and will often share his or her code on open developer websites such as GitHub, to stake the organization's claim that it had a particular idea as of a certain date. Unfortunately, that "claim" alone has little competitive value, and any sense of protection is not well-founded. Keeping this in mind, there are four fundamental problems with the practice of posting one's white paper in this manner.

"Protecting features of a full-scale blockchain-based product as trade secrets is often impractical, though, in large part because most blockchains extend beyond the boundaries of a single organization."

First, we have the same issues as the poor-man's patent with regard to achieving actual patent rights. Although many developers are primarily concerned with defending themselves against future infringement allegations, and they are less concerned with obtaining patent rights to exclude others from making the invention, investors may want to prevent others from copying the functionality of the organization's systems. The "poor-man's patent" strategy certainly does nothing to achieve patent protection and may lead to a complete loss of any potentially patentable subject matter that the organization may have otherwise enjoyed.

Second, this practice, unlike the poor man's copyright, may have the effect of completely throwing away any possibility of securing effective patent coverage. If a developer fails to file any patent application, they will certainly have no patent protection. Further, while publishing the white paper would prevent others from later patenting subject matter described therein, it would not prevent others from patenting improvements to that technology, effectively blocking the original innovator's optimal commercialization of the technology.

Third, this practice provides a clear roadmap to current patent holders who might believe that this new blockchain-based "invention" infringes their prior patent rights. Rather than providing protection, a poor man's patent can bring unwanted attention and potential liability to the new blockchain developer who might otherwise have gone unnoticed if he or she had not publicly posted the white paper or code. Some of this risk can be avoided

by the developer commissioning a freedom-to-operate search early in the development process, but in our experience, developers rarely even consider such a search.

Fourth, this practice invites other developers and competitors to manipulate the code to create their own work, which they might include in their own applications, potentially creating a competitor who got to skip the work and expense of developing the idea for themselves. While sharing the fruits of one's labors is friendly, it does not help the organization succeed in a fast-moving, competitive landscape.

Industry Trend: Defensive Patents

A more beneficial industry trend is seeking a "defensive patent." This involves a developer patenting his or her innovations, but purely as a preventative measure.[19] The developer never plans to pursue others for infringing their patents, but rather intends to use the patent as a bargaining chip. This strategy has led to multiple "defensive patent license" cooperatives, where developers pool their collective patents for all others in the pool to use.[20]

Other IP Considerations

Trademarks

Generally speaking, a trademark is any word, name, symbol, or device, or any combination thereof, used by a person to identify and distinguish his or her goods from those manufactured or sold by others and to indicate the source of the goods, even if that source is unknown.[21] Trademark rights vest when a mark is used in connection with goods and services, and as an indicator of the source of those same goods and services. These rights are afforded to the mark user against *subsequent* users (but not already-existing users) in the specific geographic market(s) where the mark is used. This bundle of rights is often referred to as "common law" trademark rights, and no registration is required to obtain them. One can obtain additional rights, putting other potential users on-presumptive notice of this mark and thereby extending these same rights to every U.S. state and jurisdiction, by registering the mark with one or more states and the USPTO.

Although neither an organization's white paper nor its computer code may serve as a source identifier, a blockchain organization's name, the name of its token, or an abbreviation of the same may become a protected trademark. However, developing trademark rights in an abbreviated name for its token, should be done cautiously to avoid consequences adverse to a client's objectives.

Some organizations plan to issue a token that will be considered a security by the U.S. Security Exchange Commission (SEC), while other organizations seek to issue a utility token, which often falls outside of SEC regulation. Regardless of the organization's intent on this point, if the organization plans to list the token on an exchange or anticipates others will do so, the SEC may consider the token a speculative investment and, thus, a security. If the organization also applied for trademark protection of abbreviated names for that token, characterizing the abbreviated name as a "ticker symbol," it could bolster the SEC's argument that the token is a security and the abbreviation is a "ticker symbol" like those that refer to stock. Therefore, caution should be used when applying for trademark protection of abbreviated names for a token, and, even without an application, in referring to the mark as a "ticker symbol" to promote its use in conjunction with a cryptocurrency exchange.

Trade Secrets

Some developers will opt for trade secret protection for their works. A trade secret is information that (i) is not generally known to the public, (ii) confers economic benefit to its holders because the information is not publicly known, and (iii) is the subject of reasonable efforts by the holder to maintain its secrecy. Although trade secret protection is often appropriate during early development of a blockchain-based technology, trade secrets are only protected so long as they *stay* a secret. For the information to have and maintain "trade secret" status, the owner must employ reasonable measures to protect that information from losing its secrecy. To that end, organizations working with outside developers should seek early IP assignments in their NDAs and contractor agreements, as discussed above, and further establish clear criteria for developers to follow for handling and safeguarding trade secrets.

Protecting features of a full-scale blockchain-based product as trade secrets is often impractical, though, in large part because most blockchains extend beyond the boundaries of a single organization. Since many blockchain applications rely on network nodes to process transactions on the blockchain, the code must be shared with those nodes. This process necessarily puts the code in the hands of many outside parties and exposes the code to be used, seen, or shared by parties outside of the developer's control. Unless the developer plans to offer a private blockchain and maintain contractual agreements with the operator of each network node to obligate those operators to keep certain trade secrets confidential, trade secret protection has limited application to blockchain technologies.

Conclusion

Blockchains and cryptocurrencies have experienced booming growth in just the past few years and look to change the way many industries operate in the years to come. Despite the rapid growth and bright future, however, blockchain organizations often cut spending on legal fees, and traditional approaches to IP protection may not fit the mold. An intentional, even cautious approach to managing IP rights and risks, coupled with consideration for industry peculiarities, can yield great, cost-effective results for developers.

Endnotes

1. *See Cryptocurrency Market Capitalizations: All Cryptocurrencies*, Coin Market Cap (March 18, 2018), www.coinmarketcap.com/all/views/all (showing total market capitalization of $296,025,148,676).
2. *See generally Alice Corp. v. CLS Bank Int'l*, 573 U.S. __, 134 S. Ct. 2347 (2014) (setting a two-step process for determining patent eligibility for software inventions).
3. *Id.* at 2354.
4. *Id.* at 2355-56 (citing *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, 566 U.S. __, 132 S.Ct. 1289, 1294-97 (2012); *Bilski v. Kappos*, 561 U.S. 593, 611 (2010); *Diamond v. Diehr*, 450 U.S. 175, 187 (1981)).
5. *Alice Corp.*, 134 S. Ct. at 2357.
6. *Cf. Chamberlain Group, Inc. v. Linear LLC*, 114 F. Supp. 3d 614, 627 (N.D. Ill. 2015) (validating a claimed invention that tied a garage door opener system to a computer network to "do new things like provide for remote monitoring and control of the garage door opener"), *with Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350, 1354, 135 (D.C. Cir. 2017) (affirming the district court's ruling that claimed inventions in collecting and monitoring power grid data sources in real time were invalid because the inventions were directed at an abstract idea and not sufficiently transformative).
7. *See Enfish v. Microsoft*, 822 F.3d 1327, 1337 (Fed. Cir. 2016) ("Here, the claims are not simply directed to any form of storing tabular data, but instead are specifically directed to a self-referential table for a computer database.").
8. *See DDR Holdings, LLC v. Hotels.com, L.P. et. al.*, 773 F.3d 1245, 1257 (Fed. Cir. 2014) (finding valid a claimed invention that "addresses a business challenge (retaining website visitors) that is particular to the Internet").
9. Leahy-Smith America Invents Act, 35 U.S.C. § 3 (2011).
10. 17 U.S.C. § 102 (2010); *Apple Computer, Inc. v. Franklin Computer Corp.*, 714 F.2d 1240, 1247 (3d Cir. 1983).
11. 17 U.S.C. §101 (2010).
12. 17 U.S.C. § 103 (2010).
13. *See Board of Trustees of Leland Stanford Junior University v. Roche Molecular Systems, Inc.*, 563 U.S. 776, 786 (2011) (holding that the language "agree to assign" in the agreement that Stanford had Holodniy sign was merely a promise to assign his invention rights to Stanford at some undetermined future point, and did not presently assign the rights upon execution of the agreement).
14. *See* David Mikkelson, *Poor Man's Copyright: Can you effectively copyright your work by mailing a copy of it to yourself?*, Snopes (Nov. 29, 2009), https://www.snopes.com/fact-check/poor-mans-copyright.
15. *See generally FAQ's: Copyright in General*, U.S. Copyright Office, available at https://www.copyright.gov/help/faq/faq-general.html (last visited Mar. 13, 2018).
16. *See, e.g.*, *Smith v. State*, 901 N.Y.S.2d 902, *8 (N.Y. Ct. Cl. July 14, 2009); *Barefoot v. Goulian*, 2010 WL 2696760, *3 (E.D. N.C. July 7, 2010); *Swensen v. Bender*, 2008 WL 2382757 (D. Minn. Feb. 22, 2008), rev'd, 764 N.W.2d 596 (Minn. Ct. App. 2009).
17. *See* Kirk Teska, *The Poor Man's Patent*, IEEE Spectrum (Aug. 1, 2008), https://spectrum.ieee.org/at-work/innovation/the-poor-mans-patent.
18. Leahy-Smith America Invents Act, 35 U.S.C. § 3 (2011).
19. *See Defensive Patent*, Techopedia, https://www.techopedia.com/definition/28565/defensive-patent (last visited Mar. 13, 2018) ("A defensive patent is a patent that is used with the primary intention of defending a company against patent infringement lawsuits.").
20. *See Defensive Patent License: Troll Proofed. Innovation Protected*, Defensive Patent Alliance, https://defensivepatentlicense.org/ (last visited Mar. 13, 2018); *Blockstream's Defensive Patent Strategy*, Blockstream, https://blockstream.com/about/patent_pledge/ (last updated Apr. 24, 2017); *Start a Blockchain Patent Sharing Era*, Blockchain IP Foundation, http://www.bpsa.io/ (last visited Mar. 13, 2018).
21. 15 U.S.C. § 1127 (2006).

Authored by Matthew R. Schantz, Member, and Jeffery T. Gorham, Senior Associate, of Frost Brown Todd, LLC's Blockchain and Digital Currency team. **Special thanks to fellow Blockchain and Digital Currency team member Kacy Joy for her support in drafting this article.**